

National Cyber Alert System

Cyber Security Bulletin SB09-146

[Archive](#)

Vulnerability Summary for the Week of May 18, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities (CVSS Score: 7.0 .. 10.0)					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
26th_avenue -- bspeak	SQL injection vulnerability in index.php in 26th Avenue bSpeak 1.10 allows remote attackers to execute arbitrary SQL commands via the forumid parameter in a post action.	2009-05-22	7.5	CVE-2009-1747 BID MILWoRM SECUNIA	
2daybiz -- business_community_script	SQL injection vulnerability in admin/member_details.php in 2daybiz Business Community Script allows remote attackers to execute arbitrary SQL commands via the mid parameter.	2009-05-16	7.5	CVE-2009-1651 BID MILWoRM SECUNIA OSVDB	
2daybiz -- business_community_script	admin/adminaddeditdetails.php in Business Community Script does not properly restrict access, which allows remote attackers to gain privileges and add administrators via a direct request.	2009-05-16	7.5	CVE-2009-1652 BID MILWoRM SECUNIA OSVDB	
armorlogic -- profense_web_application_firewall	Armorlogic Profense Web Application Firewall before 2.2.22, and 2.4.x before 2.4.4, has a default root password hash, and permits password-based root logins over SSH, which makes it easier for remote attackers to obtain access.	2009-05-21	10.0	CVE-2009-1745 BUGTRAQ	

avg -- antivirus	The AVG parsing engine 8.5.323, as used in multiple AVG anti-virus products including Anti-Virus Network Edition, Internet Security Netzwerk Edition, Server Edition für Linux/FreeBSD, Anti-Virus SBS Edition, and others allows remote attackers to bypass malware detection via a crafted (1) RAR and (2) ZIP archive.	2009-05-22	10.0	CVE-2009-1784 XF BID BUGTRAQ MISC
cisco -- ciscoworks_common_services cisco -- ciscoworks_health_and_utilization_monitor cisco -- ciscoworks_lan_management_solution cisco -- ciscoworks_qos_policy_manager cisco -- ciscoworks_voice_manager cisco -- security_manager cisco -- telepresence_readiness_assessment_manager cisco -- unified_operations_manager cisco -- unified_provisioning_manager cisco -- unified_service_monitor	Directory traversal vulnerability in the TFTP service in Cisco CiscoWorks Common Services (CWCS) 3.0.x through 3.2.x on Windows, as used in Cisco Unified Service Monitor, Security Manager, TelePresence Readiness Assessment Manager, Unified Operations Manager, Unified Provisioning Manager, and other products, allows remote attackers to access arbitrary files via unspecified vectors.	2009-05-21	10.0	CVE-2009-1161 CISCO
diangemilang -- dgnews	SQL injection vulnerability in berita.php in Dian Gemilang DGNews 3.0 Beta allows remote attackers to execute arbitrary SQL commands via the id parameter in a detail action.	2009-05-21	7.5	CVE-2009-1746 BID MILWoRM
digiye -- mypic	Directory traversal vulnerability in bom.php in MyPic 2.1 allows remote attackers to list files in arbitrary directories via a .. (dot dot) in the dir parameter.	2009-05-20	7.8	CVE-2009-1737 XF BID OSVDB SECUNIA MISC
dlink -- mpeg4_viewer_activex_control	Multiple heap-based buffer overflows in the D-Link MPEG4 Viewer ActiveX Control (csviewer.ocx) 2.11.918.2006 allow remote attackers to execute arbitrary code via a long argument to the (1) SetFilePath and (2) SetClientCookie methods. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-20	10.0	CVE-2009-1740 XF BID SECUNIA OSVDB
dutchmonkey -- dm_filemanager	Multiple SQL injection vulnerabilities in login.php in DM FileManager 3.9.2, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) Username and (2) Password fields.	2009-05-20	7.5	CVE-2009-1741 BID MILWoRM SECUNIA
electrasoft -- 32bit_ftp	Stack-based buffer overflow in ElectraSoft 32bit FTP 09.04.24 allows remote FTP servers to execute arbitrary code via a long 227 reply to a PASV command.	2009-05-18	9.3	CVE-2009-1675 XF XF BID MILWoRM
exjune -- office_message_system	exJune Office Message System 1 does not properly restrict access to (1) configure.asp and (2) addmessage2.asp, which allows remote attackers to gain privileges a direct request. NOTE: some of these details are	2009-05-22	7.5	CVE-2009-1752 XF MILWoRM SECUNIA

	obtained from third party information.		SECUNIA
f-prot -- f-prot_antivirus	Multiple FRISK Software F-Prot anti-virus products, including Antivirus for Exchange, Linux on IBM zSeries, Linux x86 File Servers, Linux x86 Mail Servers, Linux x86 Workstations, Solaris Mail Servers, Antivirus for Windows, and others, allow remote attackers to bypass malware detection via a crafted CAB archive.	2009-05-22	10.0 CVE-2009-1783 XF BID BUGTRAQ MISC
flyspeck -- flyspeck_cms	Directory traversal vulnerability in includes/database/examples/addressbook.php in Flyspeck CMS 6.8 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter.	2009-05-22	7.5 CVE-2009-1770 BID MILWoRM
flyspeck -- flyspeck_cms	index.php in Flyspeck CMS 6.8 does not require administrative authentication for the updateExistingContent action, which allows remote attackers to create or modify admin accounts via the (1) users[fullname], (2) users[email], (3) users[role_id], (4) users[username], and (5) users[password] parameters.	2009-05-22	7.5 CVE-2009-1771 BID MILWoRM
joomla -- com_gsticketsystem	SQL injection vulnerability in the GridSupport (GS) Ticket System (com_gsticketsystem) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter in a viewCategory action to index.php.	2009-05-20	7.5 CVE-2009-1736 XF BID MILWoRM
joost_horward -- catviz	Multiple directory traversal vulnerabilities in index.php in Catviz 0.4.0 Beta 1 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) webpages_form or (2) userman_form parameter.	2009-05-22	7.5 CVE-2009-1748 BID MILWoRM
maxcms -- maxcms	SQL injection vulnerability in inc/ajax.asp in MaxCMS 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter in a digg action.	2009-05-22	7.5 CVE-2009-1764 XF BID MILWoRM
microsoft -- iis	The WebDAV implementation in Microsoft Internet Information Services (IIS) 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files, via a %co%af (Unicode / character) at an arbitrary position in the URI, as demonstrated by inserting %co%af into a "/protected/" initial pathname component to bypass the password protection on the protected\ folder.	2009-05-18	7.6 CVE-2009-1676 MISC MISC MISC MISC FULLDISC FULLDISC FULLDISC
mlffat -- mlffat	SQL injection vulnerability in panel/index.php in MLFFAT 2.1 allows remote attackers to execute arbitrary SQL commands via a base64-encoded supervisor cookie.	2009-05-20	7.5 CVE-2009-1731 XF VUPEN BID MISC MISC
	Multiple directory traversal vulnerabilities in NetMechanica NetDecision TFTP Server 4.2		CVE-2009-1730

netmechanica -- netdecision_tftp_server	allow remote attackers to read or modify arbitrary files via directory traversal sequences in the (1) GET or (2) PUT command.	2009-05-20	10.0	XF BID MISC SECUNIA
nlnetlabs -- nsd	Off-by-one error in the packet_read_query_section function in packet.c in nsd 3.2.1, and process_query_section in query.c in nsd 2.3.7, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors that trigger a buffer overflow.	2009-05-22	7.8	CVE-2009-1755 CONFIRM CONFIRM CONFIRM
omnisoftsol -- vidsharepro	SQL injection vulnerability in listing_video.php in VidSharePro allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2009-05-20	7.5	CVE-2009-1734 BID MILWoRM SECUNIA
pc4arb -- pc4_uploader	code.php in PC4Arb Pc4 Uploader 9.0 and earlier makes it easier for remote attackers to conduct SQL injection attacks via crafted keyword sequences that are removed from a filter in the id parameter in a banner action, as demonstrated via the "UNIunionON" string, which is collapsed into "UNION" by the filter_sql function.	2009-05-20	7.5	CVE-2009-1742 XF VUPEN BID MILWoRM SECUNIA OSVDB
phpeasycode -- pad_site_scripts	PAD Site Scripts 3.6 allows remote attackers to bypass authentication and gain privileges as other users, including administrative privileges, by setting the authuser cookie parameter to a valid username.	2009-05-20	7.5	CVE-2009-1739 XF BID MILWoRM SECUNIA
pinnaclesys -- pinnacle_studio	Directory traversal vulnerability in InstallHFZ.exe 6.5.201.0 in Pinnacle Hollywood Effects 6, a module in Pinnacle Systems Pinnacle Studio 12, allows remote attackers to create and overwrite arbitrary files via a filename containing a ..\ (dot dot backslash) sequence in a Hollywood FX Compressed Archive (.hfz) file. NOTE: this can be leveraged for code execution by decompressing a file to a Startup folder. NOTE: some of these details are obtained from third party information.	2009-05-20	9.3	CVE-2009-1743 XF BID BUGTRAQ MILWoRM SECUNIA MISC OSVDB
rahul -- ctorrent rahul -- dtorrent	Stack-based buffer overflow in the btFiles::BuildFromMI function (trunk/btfiles.cpp) in Enhanced CTorrent (aka dTorrent) 3.3.2 and probably earlier, and CTorrent 1.3.4, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a Torrent file containing a long path.	2009-05-22	9.3	CVE-2009-1759 BID MLIST CONFIRM
realtywebware -- realty_web-base	SQL injection vulnerability in list_list.php in Realty Webware Technologies Web-Base 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-05-22	7.5	CVE-2009-1751 XF BID MILWoRM
	PHP remote file inclusion vulnerability in			CVE-2009-

roboform -- frax.dk_php_recommend	admin.php in Frax.dk Php Recommend 1.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the form_include_template parameter.	2009-05-22	7.5	1779 VUPEN BID MILWoRM
roboform -- frax.dk_php_recommend	admin.php in Frax.dk Php Recommend 1.3 and earlier does not require authentication when the user password is changed, which allows remote attackers to gain administrative privileges via modified form_admin_user and form_admin_pass parameters.	2009-05-22	10.0	CVE-2009-1780 VUPEN BID MILWoRM
roboform -- frax.dk_php_recommend	Static code injection vulnerability in admin.php in Frax.dk Php Recommend 1.3 and earlier allows remote attackers to inject arbitrary PHP code into phpre_config.php via the form_aula parameter.	2009-05-22	7.5	CVE-2009-1781 VUPEN BID MILWoRM
sun -- jre	The Deployment Toolkit ActiveX control in deploytk.dll 6.0.130.3 in Sun Java SE Runtime Environment (aka JRE) 6 Update 13 allows remote attackers to (1) execute arbitrary code via a .jnlp URL in the argument to the launch method, and might allow remote attackers to launch JRE installation processes via the (2) installLatestJRE or (3) installJRE method.	2009-05-18	9.3	CVE-2009-1672 XF MISC BID MILWoRM
sun -- opensolaris	Unspecified vulnerability in the Solaris Secure Digital slot driver (aka sdhost) in Sun OpenSolaris snv_105 through snv_108 on the x86 platform allows local users to gain privileges or cause a denial of service (filesystem or memory corruption) via unknown vectors.	2009-05-22	7.2	CVE-2009-1763 BID SUNALERT
surat_kabar -- phpwebnews	SQL injection vulnerability in bukutamu.php in phpWebNews 0.2 allows remote attackers to execute arbitrary SQL commands via the det parameter.	2009-05-22	7.5	CVE-2008-6812 XF BID MILWORM
surat_kabar -- phpwebnews	SQL injection vulnerability in index.php in phpWebNews 0.2 MySQL Edition allows remote attackers to execute arbitrary SQL commands via the id_kat parameter.	2009-05-22	7.5	CVE-2008-6813 XF BID MILWoRM
xerox -- workcentre	Xerox WorkCentre and WorkCentre Pro 232, 238, 245, 255, 265, 275; and WorkCentre 5632, 5638, 5645, 5655, 5665, 5675, 5687, 7655, 7656, and 7675 allows remote attackers to execute arbitrary commands via unknown attack vectors, aka "command injection vulnerability."	2009-05-16	10.0	CVE-2009-1656 CONFIRM VUPEN

[Back to top](#)**Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Directory traversal vulnerability in plugins/ddb/foot.php in Strawberry 1.1.1 allows remote attackers to include and execute arbitrary			CVE-2009-

	local files via a .. (dot dot) in the file parameter to example/index.php. NOTE: this was originally reported as an issue affecting the do parameter, but traversal with that parameter might depend on a modified example/index.php. NOTE: some of these details are obtained from third party information.	2009-05-22	6.8	1774 XF BID MILWoRM SECUNIA
2daybiz -- template_monster_clone	admin/edituser.php in 2daybiz Template Monster Clone does not require administrative authentication, which allows remote attackers to modify arbitrary accounts via the (1) loginname, (2) password, (3) email, (4) firstname, or (5) lastname parameter.	2009-05-22	5.0	CVE-2009-1767 XF BID MILWoRM SECUNIA
activecollab -- activecollab	Cross-site scripting (XSS) vulnerability in activeCollab 2.1 Corporate allows remote attackers to inject arbitrary web script or HTML via the re_route parameter to the login script.	2009-05-22	4.3	CVE-2009-1772 BID SECUNIA MISC
activecollab -- activecollab	activeCollab 2.1 Corporate allows remote attackers to obtain sensitive information via an invalid re_route parameter to the login script, which reveals the installation path in an error message.	2009-05-22	5.0	CVE-2009-1773 BID SECUNIA MISC
armorlogic -- profense_web_application_firewall	Armorlogic Profense Web Application Firewall before 2.2.22, and 2.4.x before 2.4.4, does not properly implement the "negative model," which allows remote attackers to conduct cross-site scripting (XSS) attacks via a modified end tag of a SCRIPT element.	2009-05-21	4.3	CVE-2009-1593 XF MLIST BID BUGTRAQ
armorlogic -- profense_web_application_firewall	Armorlogic Profense Web Application Firewall before 2.2.22, and 2.4.x before 2.4.4, does not properly implement the "positive model," which allows remote attackers to bypass certain protection mechanisms via a %oA (encoded newline), as demonstrated by a %oA in a cross-site scripting (XSS) attack URL.	2009-05-21	6.8	CVE-2009-1594 XF MLIST BID BUGTRAQ MISC
bigace -- bigace_cms	SQL injection vulnerability in the new user registration feature in BigACE CMS 2.5, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-05-22	6.8	CVE-2009-1778 CONFIRM CONFIRM
bitweaver -- bitweaver	Multiple static code injection vulnerabilities in the saveFeed function in rss/feedcreator.class.php in Bitweaver 2.6 and earlier allow (1) remote authenticated users to inject arbitrary PHP code into files by placing PHP sequences into the account's "display name" setting and then invoking boards/boards_rss.php, and might allow (2) remote attackers to inject arbitrary PHP code into files via the HTTP Host header in a request to boards/boards_rss.php.	2009-05-18	6.5	CVE-2009-1677 XF MILWoRM SECUNIA
easy-scripts -- answer_and_question_script	Cross-site scripting (XSS) vulnerability in questiondetail.php in Easy Scripts Answer and Question Script allows remote attackers to inject arbitrary web script or HTML via the questionid parameter.	2009-05-16	4.3	CVE-2009-1654 BID MILWoRM SECUNIA OSVDB

easy-scripts -- answer_and_question_script	Multiple SQL injection vulnerabilities in myaccount.php in Easy Scripts Answer and Question Script allow remote authenticated users to execute arbitrary SQL commands via the (1) user name (userid parameter) and (2) password.	2009-05-16	6.5	CVE-2009-1655 BID MILWORM SECUNIA OSVDB
easy-scripts -- answer_and_question_script	myaccount.php in Easy Scripts Answer and Question Script allows remote attackers to remove arbitrary user accounts via a modified userid parameter without specifying any additional fields.	2009-05-18	6.4	CVE-2009-1665 XF MILWORM OSVDB
f-secure -- f-secure_anti-virus	Multiple F-Secure anti-virus products, including Anti-Virus for Microsoft Exchange 7.10 and earlier; Internet Gatekeeper for Windows 6.61 and earlier, Windows 6.61 and earlier, and Linux 2.16 and earlier; Internet Security 2009 and earlier, Anti-Virus 2009 and earlier, Client Security 8.0 and earlier, and others; allow remote attackers to bypass malware detection via a crafted (1) ZIP and (2) RAR archive.	2009-05-22	6.8	CVE-2009-1782 XF VUPEN SECTRACK SECTRACK SECTRACK BID CONFIRM SECUNIA
hp -- system_management_homepage	Cross-site scripting (XSS) vulnerability in HP System Management Homepage (SMH) before 3.0.1.73 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-05-19	4.3	CVE-2009-1418 SECTRACK HP HP
ibm -- websphere_partner_gateway	IBM WebSphere Partner Gateway (WPG) 6.1.0 before 6.1.0.1 and 6.1.1 before 6.1.1.1 allows remote authenticated users to obtain sensitive information via vectors related to the "schema DB2 instance id" and the bgarchive (aka the archiver script).	2009-05-21	4.0	CVE-2009-0897 AIXAPAR
jalal_aldeen_omary -- ramazaitencms0.9.7.8 jalal_aldeen_omary -- ramazaitencms0.9.8	Directory traversal vulnerability in download.php in Rama Zaiten CMS 0.9.8 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter.	2009-05-22	6.8	CVE-2009-1768 XF VUPEN BID MILWORM SECUNIA OSVDB
joost_horward -- catviz	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Catviz 0.4.0 beta 1 allow remote attackers to inject arbitrary web script or HTML via the (1) userman_form and (2) webpages_form parameters.	2009-05-22	4.3	CVE-2009-1749 BID MILWORM
matt_wright -- formmail	Multiple cross-site scripting (XSS) vulnerabilities in FormMail.pl in Matt Wright FormMail 1.92, and possibly earlier, allow remote attackers to inject arbitrary web script or HTML via javascript: URIs in the (1) request and (2) return_link_url parameters.	2009-05-22	4.3	CVE-2009-1776 MISC BUGTRAQ SECUNIA
matt_wright -- formmail	CRLF injection vulnerability in FormMail.pl in Matt Wright FormMail 1.92, and possibly earlier, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the redirect parameter.	2009-05-22	5.0	CVE-2009-1777 MISC BUGTRAQ SECUNIA
	Cross-site scripting (XSS) vulnerability in the WebAccess login page (aka gw/webacc) in Novell	2009-05-22		CVE-2009-

novell -- groupwise	GroupWise 7.x before 7.03 HP3 and 8.x before 8.0 HP2 allows remote attackers to inject arbitrary web script or HTML via the User.lang parameter.	2009-05-22	4.3	1635 CONFIRM
novell -- groupwise	Multiple cross-site scripting (XSS) vulnerabilities in the WebAccess login page (aka gw/webacc) in Novell GroupWise 7.x before 7.03 HP2 allow remote attackers to inject arbitrary web script or HTML via the (1) GWAP.version or (2) User.Theme (aka User.Theme.index) parameter.	2009-05-22	4.3	CVE-2009-1762 CONFIRM
ntp -- ntp	Stack-based buffer overflow in the crypto_recv function in ntp_crypto.c in ntpd in NTP before 4.2.4p7 and 4.2.5 before 4.2.5p74, when OpenSSL and autokey are enabled, allows remote attackers to execute arbitrary code via a crafted packet containing an extension field.	2009-05-19	6.8	CVE-2009-1252 CERT-VN
ocsinventory-ng -- ocs_inventory_ng	The web interface in OCS Inventory NG 1.01 generates different error messages depending on whether a username is valid, which allows remote attackers to enumerate valid usernames.	2009-05-22	5.0	CVE-2009-1769 BID MISC SECUNIA CONFIRM
omnisoftsol -- vidsharepro	Cross-site scripting (XSS) vulnerability in search.php in VidSharePro allows remote attackers to inject arbitrary web script or HTML via the searchtxt parameter. NOTE: some of these details are obtained from third party information.	2009-05-20	4.3	CVE-2009-1735 BID MILWoRM SECUNIA
omnisoftsol -- vidsharepro	Unrestricted file upload vulnerability in VidSharePro allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via unspecified vectors.	2009-05-22	6.0	CVE-2009-1750 XF BID MILWoRM
openssl -- openssl openssl_project -- openssl	The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."	2009-05-19	5.0	CVE-2009-1377 CONFIRM MLIST CONFIRM
openssl -- openssl openssl_project -- openssl	Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."	2009-05-19	5.0	CVE-2009-1378 CONFIRM MLIST CONFIRM
openssl -- openssl	Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allows remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact via a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate.	2009-05-19	5.0	CVE-2009-1379 MISC XF VUPEN SECTRACK MLIST CONFIRM
pinnaclesys -- pinnacle_studio	InstallHFZ.exe 6.5.201.0 in Pinnacle Hollywood Effects 6, a module in Pinnacle Systems Pinnacle Studio 12, allows remote attackers to cause a	2009-05-22	4.3	CVE-2009-1744

	denial of service (application crash) via a crafted Hollywood FX Compressed Archive (.hfz) file.	"0		MILWoRM
pluck-cms -- pluck	Multiple directory traversal vulnerabilities in pluck 4.6.2, when register_globals is enabled, allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the langpref parameter to (1) data/modules/contactform/module_info.php, (2) data/modules/blog/module_info.php, and (3) data/modules/albums/module_info.php, different vectors than CVE-2008-3194.	2009-05-22	6.8	CVE-2009-1765 BID MILWoRM SECUNIA
richard_ellerbrock -- ipplan	Cross-site scripting (XSS) vulnerability in admin/usermanager in IPlan 4.91a allows remote attackers to inject arbitrary web script or HTML via the grp parameter.	2009-05-20	4.3	CVE-2009-1732 BID SECUNIA MISC
richard_ellerbrock -- ipplan	Cross-site request forgery (CSRF) vulnerability in IPlan 4.91a allows remote attackers to hijack the authentication of administrators for requests that (1) change the password, (2) add users, or (3) delete users via unknown vectors.	2009-05-20	6.8	CVE-2009-1733 SECUNIA MISC
squirrelmail -- imap_general.php squirrelmail -- squirrelmail	The map_yp_alias function in functions/imap_general.php in SquirrelMail before 1.4.19-1 on Debian GNU/Linux, and possibly other operating systems and versions, allows remote attackers to execute arbitrary commands via shell metacharacters in a username string that is used by the ypmatch program. NOTE: this issue exists because of an incomplete fix for CVE-2009-1579.	2009-05-22	6.8	CVE-2009-1381 BUGTRAQ
sun -- solaris	The kernel in Sun Solaris 9 allows local users to cause a denial of service (panic) by calling fstat with a first argument of AT_FDCWD.	2009-05-18	4.9	CVE-2009-1673 VUPEN SUNALERT CONFIRM
sun -- java_system_communications_express	Multiple cross-site scripting (XSS) vulnerabilities in Sun Java System Communications Express 6 2005Q4 (aka 6.2) and 6.3 allow remote attackers to inject arbitrary web script or HTML via (1) the abperson_displayName parameter to uwc/abs/search.xml in the Add Contact implementation in the Personal Address Book component or (2) the temporaryCalendars parameter to uwc/base/UWCMain.	2009-05-21	4.3	CVE-2009-1729 BID BID BUGTRAQ SUNALERT CONFIRM
teozkr -- lightopencms	SQL injection vulnerability in index.php in LightOpenCMS 0.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-05-22	6.4	CVE-2009-1766 MILWoRM
transmissionbt -- transmission	Cross-site request forgery (CSRF) vulnerability in Transmission 1.5 before 1.53 and 1.6 before 1.61 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2009-05-22	6.8	CVE-2009-1757 CONFIRM MLIST
	Multiple cross-site scripting (XSS) vulnerabilities in Ulteo Open Virtual Desktop 1.0 allow remote attackers to inject arbitrary web script or HTML via the id parameter to (1)			CVE-2009-1777

ulteo -- open_virtual_desktop	admin/applications.php, (2) admin/appsgroup.php, (3) admin/users.php, (4) admin/usersgroup.php, and (5) admin/tasks.php; (6) show parameter to admin/logs.php; and (7) mode parameter to admin/configuration-partial.php. NOTE: some of these details are obtained from third party information.	2009-05-22	4.3	1/5 CONFIRM BID MISC SECUNIA
ulteo -- open_virtual_desktop	Cross-site scripting (XSS) vulnerability in Ulteo Open Virtual Desktop 1.0 allows remote attackers to inject arbitrary web script or HTML via the error parameter to header.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-22	5.0	CVE-2009-1785 MISC
xen -- xen	The hypervisor_callback function in Xen, possibly before 3.4.0, as applied to the Linux kernel 2.6.30-rc4, 2.6.18, and probably other versions allows guest user applications to cause a denial of service (kernel oops) of the guest OS by triggering a segmentation fault in "certain address ranges."	2009-05-22	5.0	CVE-2009-1758 MLIST MLIST

[Back to top](#)**Low Vulnerabilities (CVSS Score: 0.0 .. 3.9)**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
drupal -- feed_block	Cross-site scripting (XSS) vulnerability in Feed Block 6.x-1.x before 6.x-1.1, a module for Drupal, allows remote authenticated users with administrator feed permissions to inject arbitrary web script or HTML via unspecified vectors in "aggregator items."	2009-05-20	3.5	CVE-2009-1738 CONFIRM CONFIRM
emn -- coccinelle	Coccinelle 0.1.7 allows local users to overwrite arbitrary files via a symlink attack on an unspecified "result file."	2009-05-22	3.6	CVE-2009-1753 CONFIRM
simone_rota -- slim_simple_login_manager	SLiM Simple Login Manager 1.3.0 includes places the X authority magic cookie (mcookie) on the command line when invoking xauth from (1) app.cpp and (2) switchuser.cpp, which allows local users to access the X session by listing the process and its arguments.	2009-05-22	2.1	CVE-2009-1756 XF BID MLIST SECUNIA OSVDB CONFIRM

[Back to top](#)

Last updated May 26, 2009

 Print This Document